



CVE-2019-3462

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-3462
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-28 21:29:00 UTC
Updated	2023-11-07 03:09:00 UTC
Description	Incorrect sanitation of the 302 redirect field in HTTP transport method of apt versions 1.4.8 and earlier can lead to content i

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Application	Debian	Advanced Package Tool	All	All	All	All
Application	Debian	Advanced Package Tool	All	All	All	All
Application	Debian	Advanced Package Tool	All	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

Application	Netapp	Active Iq	-	All	All	All
Application	Netapp	Active Iq	-	All	All	All
Application	Netapp	Element Software	-	All	All	All
Application	Netapp	Element Software	-	All	All	All

References

Reference	Source	Link	Tags
CVE-2019-3462 APT Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Third Party Adviso
[SECURITY] [DLA 1637-1] apt security update	MLIST	lists.debian.org	Mailing List, Vendc
Debian apt CVE-2019-3462 Remote Code Execution Vulnerability	BID	www.securityfocus.com	Third Party Adviso
[SECURITY] [DLA 1637-1] apt security update (amended)	MLIST	lists.debian.org	Mailing List, Vendc
Pony Mail!		lists.apache.org	
USN-3863-2: APT vulnerability Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party Adviso
USN-3863-1: APT vulnerability Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party Adviso
Pony Mail!	MLIST	lists.apache.org	Mailing List, Vendc
Debian -- Security Information -- DSA-4371-1 apt	DEBIAN	www.debian.org	Patch, Vendor Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report